Homeland Security

August 24, 2011

FISM 11-01

FEDERAL INFORMATION SECURITY MEMORANDUM FOR THE HEADS OF EXECUTIVE BRANCH CIVILIAN DEPARTMENTS AND AGENCIES

FROM: Roberta G. Stempfley, Acting Assistant Secretary, Office of Cybersecurity & Communications, Department of Homeland Security

SUBJECT: Announcing Trusted Internet Connections (TIC) Reference Architecture v2.0

This Federal Information Security Memorandum (FISM)[1] informs the heads of executive branch civilian departments and agencies of the revised TIC Reference Architecture v2.0.

The TIC Reference Architecture v2.0 introduces new, and clarifies existing, mandatory critical capabilities. In addition to mandatory critical capabilities, the TIC Reference Architecture v2.0 includes recommended capabilities based on evolving technologies and threats. Recommended capabilities are considered desirable, but do not have well-defined standards due to evolving technologies, threats, or requirements. TIC Access Providers (TICAPs) and Managed Trusted Internet Protocol Service (MTIPS) providers should plan for recommended TIC capabilities, and implement them as federal and industry standards are more fully defined. In the next revision of the TIC Reference Architecture, these recommended capabilities are expected to become mandatory critical capabilities.

The TIC Reference Architecture v2.0 and additional information is available on the OMB MAX Portal (requires a .GOV or .MIL e-mail address to register):
https://max.omb.gov/community/display/Egov/Trusted+Internet+Connections

The TIC Reference Architecture v2.0 applies to:

- agencies designated as TICAPs;
- commercial carriers designated as MTIPS providers; and
- all federal executive branch civilian agencies procuring Networx MTIPS or using TICAP services.

Agencies are reminded they still must complete the following previously established TIC Reference Architecture v1.0 Milestones.

Previous TIC v1.0 Milestones:

January 1, 2011. Approved TICAP departments and agencies and Networx MTIPS providers will schedule their next TIC Compliance Validation (TCV)/Cybersecurity Compliance Validation

[1] The Department of Homeland Security issues Federal Information Security Memoranda to inform federal departments and agencies of their responsibilities, required actions, and effective dates to achieve federal information security policies.

(CCV) annual assessments with the Department of Homeland Security's Federal Network Security Branch, Compliance & Assurance Program.

January 31, 2011. All other executive branch civilian departments and agencies route all external connections, including to the Internet, through a TIC v1.0-compliant TICAP or MTIPS provider.

Individual Dates. Approved TICAP departments and agencies achieve 100% technical capabilities and 100% consolidation of external connections, including those to the Internet, according to their individual TIC Plans of Actions & Milestones (POA&Ms) submitted to the TIC Program Office.

DHS issues this memorandum pursuant to the following authorities:

- The Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541-3549,
- Office of Management and Budget's (OMB) M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and DHS* (assigning to DHS certain responsibilities under FISMA), and
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23, *Comprehensive National Cybersecurity Initiative* (especially paragraphs 15 and 25).

Additional relevant documents include:

- OMB M-08-05: *Implementation of Trusted Internet Connections (TIC)*
- OMB M-08-16: *Guidance for Trusted Internet Connection Statement of Capability (SOC) Form*
- OMB M-08-27: *Guidance for Trusted Internet Connection (TIC) Compliance*
- OMB M-09-32: *Update on the Trusted Internet Connections Initiative*

For additional information or questions, please contact Sean Donelan, TIC Program Management Office, Federal Network Security Branch, Department of Homeland Security at tic@dhs.gov or by telephone 703-235-5122.